SELECTED TOPICS IN ADVANCED ELECTRONICS

Edited by

Khalid A. S. Al-Khateeb

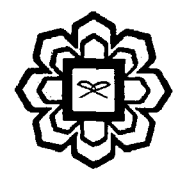
IIUM Press

INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA

SELECTED TOPICS IN
ADVANCED ELECTRONICS

Edited by

Khalid A. S. Al-Khateeb



IIUM Press
International Islamic University Malaysia
2011

Published by:
IIUM Press
International Islamic University Malaysia

First Edition, 2011
©IIUM Press, IIUM

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without any prior written permission of the publisher.

Perpustakaan Negara Malaysia Cataloguing-in-Publication Data

Khalid A. S. Al-Khateeb: Selected Topics in Advanced Electronics

ISBN: 978-967-418-153-6

Member of Majlis Penerbitan Ilmiah Malaysia – MAPIM
(Malaysian Scholarly Publishing Council)

Printed by :
IIUM PRINTING SDN.BHD.
No. 1, Jalan Industri Batu Caves 1/3
Taman Perindustrian Batu Caves
Batu Caves Centre Point
68100 Batu Caves
Selangor Darul Ehsan
Tel: +603-6188 1542 / 44 / 45 Fax: +603-6188 1543
EMAIL: iiumprinting@yahoo.com

SELECTED TOPICS IN

ADVANCED ELECTRONICS

CONTENTS

CHAPTER 7

THEORY OF QUANTUM CRYPTOGRAPHY

By

[1]Ali Sallami and [2]Khalid A. S. Al-Khateeb
[1]Department of Science in Engineering
[2]Department Electrical and Computer Engineering
Kulliyyah of Engineering
International Islamic University Malaysia

Synopsis

The world has never witnessed a technological revolution as it has with Computers and Communications. However, this great revolution is hindered from achieving its full potential by intruders and eavesdroppers as well as virus and hacker invasions. Therefore, cyber security has become one of the major concerns. Users from a variety of fields, especially those which demand extremely high security such as government, commerce, banking, diplomatic and military correspondence, just to name a few require high degree of protection. They are prepared to invest millions of dollars to combat the invaders. However with the ever increasing speed and computing capacity, no sooner a secure code is developed than a counter attack is launched to break it. The most plausible security systems so far are those which rely on Quantum Mechanics (QM), which in spite of some major breakthroughs are still under development. These laws are applied to two aspects of communications security; cryptography and authentication. The technique is based on the idea that the sender (Alice) and receiver (Bob) share a random sequence of Quantum Bits (qubits). The initial step of key distribution, in which the two parties acquire the key material, must be accomplished with a high level of confidence that a third party (Eve) cannot even get partial information of the random bit sequence.